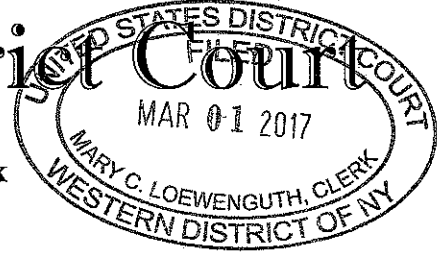


United States District Court

for the
Western District of New York



United States of America

v.

Case No. 17-MJ- 524

WILLIAM R. ROSICA

Defendant

CRIMINAL COMPLAINT

I, KEVIN PARKER, FBI, the complainant in this case, state that the following is true to the best of my knowledge and belief.

Beginning in or about March 2016 through February 28, 2017, in the County of Monroe, in the Western District of New York, the defendant violated 18 U.S.C. §§ 2261A(1)(B), 2261A(2)(B) and 1030(a)(2)(C), offenses described as follows:

the defendant, with the intent to kill, injure, harass, intimidate or place under surveillance with the intent to kill, injure, harass or intimidate, engaged in conduct and used an interactive computer service or electronic communication system of interstate commerce to engage in a course of conduct that caused or attempted to cause substantial emotional distress to another person, in violation of Title 18, U.S.C. §§ 2261A(1)(B), 2261A(2)(B); and

attempted to access a computer without authorization to obtain information from a protected computer, in violation of Title 18, U.S.C. § 1030(a)(2)(C).

SEE ATTACHED AFFIDAVIT OF KEVIN PARKER, S.A., FBI.

This Criminal Complaint is based on these facts:

☒ Continued on the attached sheet.

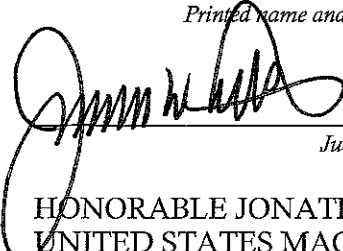
Sworn to before me and signed in my presence.

Date: March 1, 2017

City and State: Rochester, New York


Complainant's signature

KEVIN PARKER, S.A. FBI
Printed name and title


Judge's signature
HONORABLE JONATHAN W. FELDMAN
UNITED STATES MAGISTRATE JUDGE
Printed name and title

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

STATE OF NEW YORK)
COUNTY OF MONROE) SS:
CITY OF ROCHESTER)

I, Kevin Parker, being duly sworn, do depose and say:

I. INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"). I am currently assigned to the Cyber Squad, Buffalo Division, in Rochester, New York. As part of the Cyber Squad, I work on investigations relating to criminal and national security cyber intrusions. I have gained experience through training and everyday work related to these types of investigations. During my tenure with the FBI, I have also worked on other types of investigations including counterintelligence and counterterrorism. I am empowered by law to conduct investigations of, and make arrests for, offenses against the United States.

2. I am currently assigned to the investigation of a stalking and computer intrusion scheme perpetrated by William Robert Rosica (hereinafter "Rosica") in the Western District of New York.

3. This affidavit is submitted in support of a criminal complaint charging Rosica with engaging in stalking, in violation of 18 U.S.C §§ 2261A(1)(B), 2261(2)(B), and attempted to access information from protected computers in violation of 18 U.S.C. § 1030(a)(2)(C). The following information comes from my own investigation of the crimes alleged. Because

this affidavit is being submitted for the limited purpose of obtaining a criminal complaint against Rosica, and a corresponding arrest warrant, I have not included each and every fact known to me concerning this investigation.

II. PROBABLE CAUSE

4. On or about November 2016, the Buffalo FBI met with the New York State Police regarding an ongoing computer intrusion and stalking investigation. Initial discussions identified a Rochester, New York based female (initials L.M.) (hereinafter, the “victim”) that has been targeted throughout 2016 through the use of a variety of internet based mediums. Following the end of a relationship with Rosica, the victim began receiving harassing text messages, phone calls, and emails. The communications slowly escalated in both content and obfuscation techniques. In addition, the victim’s work email account and online medical system (University of Rochester’s MyChart) had numerous unauthorized access attempts. Rosica also targeted the victim’s ex-husband and co-workers. Investigation results to date have shown Rosica to use the ToR network in conjunction with other obfuscation web sites and email providers.

5. In February 2016, the victim ended a three-year relationship with Rosica. Following the end of the relationship the victim and Rosica engaged in conversations regarding the ending of the relationship. On March 3, 2016, Rosica emailed the victim with the following, “... Please consider speaking with me and allowing me the chance to make things clearer and more right with you. I know you are very upset. ...Being too quick to anger and too quick to accuse is NOT what I want to do ever again...” On March 23, 2016,

the victim received an anonymous text message which stated it was from 'trustmeiknow@yahoo.com' and included the message: "I have already provided him with all of the information he needs to know how you played him. And you wonder why you have no friends?"

6. Also on March 23, 2016, the victim received a text message from 'anonymous@textem.net' with the message: "I think he knows how you played him. Arguing and fighting to throw him off. All while you were setting up with someone else?"

7. Based on the Affiant's training and expertise combined with research associated from this investigation, your Affiant believes that 'trustmeiknow@yahoo.com' is not a real email address and was entered within a website advertising free text messaging. The website www.textem.net markets free text messaging services; any user with access to the internet can navigate to this website and enter a recipient's phone number, sending email address visible when the message is received (optional), recipient mobile carrier, and message content. Your Affiant performed a text message test on December 2, 2016, using the fake email address of 'abc@yahoo.com' and message content of 'Test'; the message was received on the Affiant's cellular phone and appeared to have been sent by 'abc@yahoo.com.' It is your Affiant's belief that text messages referenced throughout the remainder of this affidavit utilize the same or similar services and that the email addresses provided are not real nor used in traditional email communications by the target user.

8. On April 17, 2016, Rosica emailed the victim and stated the he had also been the target of harassing emails and text messages. The content of the email included the following, "I have had enough. All hours of the day, night, middle of the night. If you know who is doing this please have them stop! The last two came from lmino@yahoo.com. I have my number blocked from that one site. Thank u." The email includes six attachments of screen shots taken from a mobile phone screen; the attachments included file names appearing to be timestamps taken on April 17, 2016. The first image had a screenshot appearing to be from trustmeiknow@yahoo.com with a series of incoming text messages: "wake up and realize what it is", "whatever you do do not trust her she is lying bigtime you fool", "has she told you yet?", "she needs to tell you something soon she is hiding something from you run!!". The second image had a screenshot appearing to be from lmino@yahoo.com with a series of incoming text messages: "HA HA", "FUCK OFF!". The third image had a screenshot appearing to be from iamonit@yahoo.com with a series of incoming text messages: "she is not telling you everything. There is something going on you need to know about", "don't say you weren't warned", "sorry to trouble you but she is up to something you really need to know about", "when are you going to learn your lesson??? She is not telling you everything!", "shes lying to you". The fourth image had a screenshot appearing to be from iamonit@yahoo.com with a series of incoming text messages: "Has she told you yet? She needs to tell you something", "when will you learn?", "you need to wake up", "wake up idiot!". The fifth image had a screenshot appearing to be from iamonit@yahoo.com with a series of incoming text messages: "why are you wasting your time? She is a liar", "are you frustrated yet?", "you have been played oh so well", "she has serious issues you need to know about!!", "shes got someone over there right now". The sixth image had a screenshot

appearing to be from iamonit@yahoo.com with a series of incoming text messages: “you missed out on the good information you fool”, “you are an idiot. You deserve what you get.”, “haven’t you figured it out yet?”, “what a jerk off you are! She is playing you!!!!!!!!”, “fuck you”, “dumb fuck”.”

9. On or about May 22, 2016, the victim stated that she broke off all communications with Rosica. The victim told the FBI this was one of the first milestones in the evolution of Rosica’s behavior; one of the first turning points when she noticed the harassment and communications become more aggressive and technically sophisticated.

10. On June 3, 2016, the victim received an email sent from Rosica, the content of the email included: “I take responsibility for anything I have said or done that was misguided based on rumor, innuendo or from misplaced anger.” “I am sorry for the document I left with you because in NO WAY did I intend to imply anything from it other than your own concerns, that you have shared with me, regarding your thyroid issues. I NEVER meant that the entire document pertained to you and I should have been clearer about that. I really thought I was trying to help. Please believe that!” The document referenced by Rosica was a research paper titled, “The Thyroid and the Mind and Emotions/Thyroid Dysfunction and Mental Disorders” and was written by a Professor of Psychiatry with the University of Toronto.

11. On July 16, 2016, the victim received an email sent from Rosica, the content of the email included: “I remain deeply concerned for your well being whether you agree with

that or not. I will repeat this forever I DO NOT think you are crazy, psycho or mental... I wish I could have handled the paperwork thing differently.”

12. On August 22, 2016, the victim stated she agreed to meet, in person, with Rosica. According to the victim, Rosica stated, “I am at a cross-roads. Either I let you walk away and we live our separate lives or short of killing you, I destroy every aspect of your life. You tell me what I should do.” The victim stated her request was to be left alone and walk away. The victim identified this meeting as another milestone further increasing the intensity of harassing contact and technical sophistication.

13. On August 28, 2016 Rosica sent an email to the victim which included the following, “...And with regard to our last conversation in the park, I still remain at a cross-roads. I must protect my better interests.”

14. On September 6, 2016, the victim received multiple automated text messages from AT&T (Victim’s cellular phone provider). The text messages provided the following, “AT&T Free Msg: Your User ID is lansing862904suv. Wireless number 5856359226 can also be used to log in. Did not request? 800.ATT.2020.” Based on your Affiant’s training and expertise, this text message represents the attempted and potentially successful access of the victim’s AT&T online account.

15. On September 7, 2016, Rosica sent the victim an email with the following, “I am on the phone with the fraud department at Verizon. Since 4:05 p.m. yesterday, I have

had 17 attempts into my Verizon account. The password keeps getting reset. I have also had 24 attempts into my AOL account. Three step verification is already in place. I have had 2 attempts into my Google account (which is odd because only a handful of people know that I even use that account). Two step verification is in place. "Katy Jones" has now sent me 216 emails! One better than the other. She's one busy girl. This is all legitimate and NOT bullcrap! I have saved every message from Verizon, AOL, and Gmail. I am working diligently to find out the perpetrator and I am very close to going public with this and filing a police report if it does not stop! I am pissed, exhausted and frustrated. I do not want anyone knowing my business (which could also drag you into this). Please, if you know who is doing this, tell them to stop now! Enough is enough!" The Katy Jones referenced in the email from Rosica is a reference to the email accounts katy.jones76@yandex.com and katy.jones76@muchomail.com; Rosica is referencing emails he received directly from those accounts with alleged details of what the victim was doing. For instance, the Katy Jones accounts emailed Rosica with messages stating, "ask around shes talking all kinds of shit about you shes making you look foolish", "she is on your street right now", and "your job cant protect you". Note: Yandex is a Russian multinational technology company specializing in Internet-related services and products. Yandex operates the largest search engine in Russia with about 60% market share in that country; Yandex would be comparable to Google (and Gmail) in the United States.

16. A subpoena return for the email account katy.jones76@muchomail.com identified the following subscriber data: Name: Katy Jones, 123 Main St, Dallas, TX 75189, DoB: 1/1/76, Join Date: 7/21/2016, Total Logins: 171, and Last Login on 9/12/2016 from

IP address: 91.121.230.209. An open source lookup of the IP address identified a ToR exit node.

17. On September 8, 2016, three attempted login attempts were made into the victim's employer's email system. The IP Addresses used for the attempted access were from ToR Network exit nodes. September 8, 2016 represents the first date known in the investigation where Rosica attempted access into the victim employer's email account.

18. Throughout the month of September 2016, additional text messages were received from AT&T with similar attempted access messages as identified above. On or about the middle of September, the victim changed cellular phone numbers and online accounts; soon after switching the victim received the same AT&T automated text messages with the new online ID. Additionally, multiple additional attempts to access the victim's employer email account were made, and all were made from ToR exit nodes.

19. On or about Labor Day weekend 2016, which was on or about September 18, 2016, the victim's ex-husband and the victim spent the day at the Canal Days festival near the ex-husband's residence. The victim drove her new Honda CRV to the ex-husband's residence and parked it in the driveway. After the victim left the ex-husband's residence in the afternoon, the ex-husband checked his mobile phone and saw multiple text messages from 'Katy Jones' referencing that the victim been at the ex-husband's residence. The text messages included the following, "Tell [victim] kathy jones says hello", "I Will make sure bill knows [victim] is at your house right now", "Shes been lying to bill for months", "[victim] has told

many people you are a drunk and you abused her”, “Tell [victim] katy is sending bill a picture of her car in your driveway while she helps you with yard work”, “we tried to warn bill”.

20. On September 18, 2016, Rosica forwarded an email message to the victim. The content of the original forwarded message stated, “this is [victim’s] new car parked at her ex-husband’s house on [ex-husband address] have her explain why she is at her ex’s house when she has made it known he was abusive to her shes even helping him do yard work in her kaki shorts and grey t-shirt this was taken on sunday 9 18 aroun [*sic*] 1 pm”. The victim confirmed receiving a picture in the email that showed her new vehicle in her ex-husband’s driveway. A digital copy of the image was provided to the FBI, which showed a Honda CRV with a NY license plate matching that of the victim’s vehicle.

21. In this September 18, 2016 forwarded email, Rosica wrote the following, “When you decided to start sending things back to me with my name on them in July, that’s when I suspected you had someone else. We started talking again and I begged for you to tell me the truth and you kept lying, as is evident now. You knew I knew. I felt sorry for you because I thought you were going to kill yourself again like you did several years ago. Remember when you were in-patient psych for downing all of those phenobarbital pills??... Better yet, maybe your son needs to know just how psycho you are... Did you bring Gypsy with you to [victim ex-husband’s] today or did you leave her home in the crate again? ...Both Doctors were right about you—Borderline Personality Disorder along with Mania and Depression (although you only ever admitted to the depression). You are pathetic, PSYCHO, a LIAR, and the MOST untrustworthy person I have ever met... What would your son think

of his mother being suicidal? That is where you are headed. You have created such messes in your life that you will end up having no other option.”

22. On or about October 6, 2016, the IT Manager for the victim’s employer, was contacted by the employer’s Office Manager. The Office Manager informed the IT Manager that a user at the company had their email hacked. The IT Manager checked access logs, enabled two-factor authentication, and changed passwords. The IT Manager extracted available logs for the previous 180 days and voluntarily provided those to the NY State Police. Following the involvement of the FBI, the NY State Police then provided the FBI those historic logs. The FBI’s review of the alleged access to the victim’s email account indicated that, with a high level of confidence, no unauthorized access was obtained for the period of activity provided; all unauthorized activity was only attempted and either failed at an invalid password or stopped after a challenge question. On February 9, 2017 the IT Manager voluntarily provided the FBI with an updated analysis of attempted access into the victim’s email account; that analysis showed 282 unique unauthorized attempts beginning September 8, 2016 and ending on February 6, 2017.

23. On October 16, 2016, the victim received a text message from email account ‘sycamoreneighbor@yahoo.com’ with the message: ‘when sneaking around at night and switching and hiding vehicles, please remember to shut the lights off in your house so you don’t waste electricity’. The victim’s home residence is off a street with the name Sycamore. Based on your Affiant’s training and expertise, and the investigation to date, your Affiant

believes the email address to not be an authentic Yahoo address and was only used to harass the victim.

24. On October 19, 2016, the victim received a text message from email account 'flatchest@yahoo.com' with the message: 'watch your speed Winton or Monroe tonight? what time will you be at [victim's ex-husband] or is he coming over tonight?' Based on the Affiant's training and expertise, and the investigation to date, your Affiant believes the email address to not be an authentic Yahoo address. Further, your Affiant believes the content of the messages could only be known by physical surveillance of the victim and her residence. Your Affiant believes these messages were used to scare the victim into believing she is being followed and that the sender, not only knows where she lives, but also knows her route home.

25. On October 25, 2016, the victim received four separate text messages with references to assisting in suicide. From email address 'lightsoutonsycamore@yahoo.com', message: <http://www.mysticmadness.com/7-easiest-and-best-ways-to-commit-suicide.html>. From email address 'halfpynt72@gmail.com', message: http://www.cracked.com/article_15658_the-ten-minute-suicide-guide..html. From email address 'trailertrashliar@yahoo.com', message: <http://www.alexshalman.com/2008/08/05/10-simple-ways-to-commit-suicide/>. From email address 'loser@yahoo.com', message: <http://www.insidermonkey.com/blog/7-easiest-painless-ways-of-killing-yourself-360388/>.

26. On October 26, 2016, the victim received six unique text messages from Google with a verification code. Based on your Affiant's training and expertise, your Affiant believes these text messages were initiated based upon unauthorized access attempts into the victim's personal email account.

27. On October 29, 2016, the victim received numerous text messages. A portion of those text messages provide medical characteristics of individuals with personality disorder (for example, 'people with personality disorder are also usually very impulsive, oftentimes demonstrating self-injurious behaviors'). The remaining portion of text messages reference encouraging the victim to commit suicide. Text message from 'halfpynt72@gmail.com' to victim, message: trailer trash lying cheating psycho u ruin everything you touch liar liar psycho liar cheater cheater liar psycho go take some pills lots of them. Text message from 'halfpynt72@gmail.com' to victim, message: watching the move [sic] "me before you" twice in one week is a good sign your thinking of killing yourself again good for you do it right this time psycho. Text message from '5857336606@txt.att.net' to victim, message: watching the move [sic] "me before you" twice in one week is a good sign your thinking of killing yourself again good for you do it right this time psycho. Text message from 'halfpynt72@gmail.com' to victim, message: watch more suicide related movies then take some more of your pills. Text message from 'email@addthis.com' to victim, message: SUBJ: 99 Little Known Facts about suicide MSG: watch more suicide related movies and tell people you are not psycho and crazy take plenty more pills you are out of your mind and a liar. Text message from 'noreply@txt2day.com' to victim, message: SUBJ:Sent by IP 46.166.188.209 MSG: interesting movie selections more suicide flicks?

28. On October 30, 2016, the victim received an email from weknow@hotdak.net with the message: “anyone(everyone) knows what a liar you are you cant ever keep youre stories straight with your neighbors no need to hide in any of the garages you park in we know what you do and when you do it you get no sympathy from us you ruined our quiet neighborhood with your trailer park antics.” This was the first email the victim received from the email account weknow@hotdak.net.

29. A subpoena return for the email account weknow@hotdak.net identified the following subscriber data: Name: all knowing, 123 Main St, Rochester, NY 14605, DOB: 1/1/76, Join Date: 10/30/2016, Total Logins: 124, and Last Login on 12/18/2016 from IP address: 51.15.36.187. An open source lookup of the IP address identified a Europe based cloud storage and data provider.

30. On November 27, 2016, the victim received an email from weknow@hotdak.net with the message: “youre little “lies” werent so little after all it has unraveled all this mess people must know what a true skank you are lying filthy cheating trailer trash skank with a grossly fat ass and ankles as big as stumps are you tired yet of ruining others? Seek help or eat pills or both!”

31. On November 30, 2016, two attempts were made to remotely access the online University of Rochester MyChart account containing medical information for the victim. The attempts were identified via automated Login ID recovery emails sent to victim’s personal

email account. An interview of the victim stated she did not initiate the unauthorized attempted access but she did change her password after learning of the attempts.

32. On December 7, 2016, the victim received a phone call from Walgreens stating her prescription was ready for pick-up. After speaking with the pharmacist, victim stated that she had previously cancelled all her auto-refill prescriptions but for some reason this one was not cancelled. After picking up her prescriptions the evening of December 7, 2016, the victim received an email from weknow@hotdak.net with the message: "bout time you picked up youre psyche pills at drug store youre driving is not great either hurry home so you can go to trailvervile how does it feel deep in youre mind to know you are a skank liar? don't be surprised how many people know all of this... a suicidal skank liar so many people know that now..."

33. Also on December 7, 2016, two individuals at the victim's employer received emails from weknow@hotdak.net. The emails were sent to the Managing Partner and Operations Manager. Content of the email stated: "you need to look closer at her do not let her fool you if you talk to the right people they will tell you what you need to hear you should read some of the emails she has sent about youre firm ask the right people and you will find the truth do not be fooled!"

34. An interview with the victim's pharmacy identified a pattern of anonymous and fake phone calls inquiring about the victim's medications. The employees at the pharmacy have documented phone calls on September 26, 2016, October 20, 2016, seven

times on December 1, 2016, December 2, 2016, December 3, 2016, December 4, 2016, December 6, 2014, December 14, 2016, December 15, 2016, twice on December 16, 2016, December 29, 2016, four times on December 30, 2016, January 2, 2017, and January 4, 2017.

35. On December 13, 2016, weknow@hotdak.net sent a second email to the victim's employer's Managing Partner and Operations Manager. The content of the message included: "[victim] is creating this drama because she is mad about her bonus you should here her bad mouth you both shes hoping all this attention will make you feel sorry for her go look at her emails and see what she has sent out about both of you talk to the other firms where holly is known as the "C" word according to [victim] john is a "dirty cheating lawyer" the girls at these other firms can confirm this she has serious mental issues."

36. On December 14, 2016, the victim refilled a prescription through a Walgreens automated tool and 14 minutes later received an email from weknow@hotdak.net with the message: "you have 2 new psyche meds waiting for you hopefully this batch of pills will fix youre illness if not just take the whole bottle are these antiskank pills? ...another person found out today what a lying skank you are".

37. On December 15, 2016, weknow@hotdak.net sent a third email to the victim's employer's Operations Manager. The content of the message included: "check her emails she continues to shitalk [*sic*] you she has talked to a lot of girls from other firms about you she is looking for a new job everyday on work time she calls [Managing Partner's first name] a crook and you a "C" word every change she gets she is already crying about her bonus dont

let her fool you she creates drama so people will feel sorry for her she makes shit up all the time she is poison she has serious mental issues and is heavily medicated do not let her fool you if you want more info let me know she loves ruining lives.”

38. On December 21, 2016, the victim received an email from weknow@hotdak.net with the message: “youre plans for a new job will not go well a certain note about you has been circulated to the right people and they wont even touch youre resume they too know what a lying untrustworthy skank you are you have sent out some interesting emails over the last few months and youre boss now is not to happy be careful of the smiling face that says “dont worry [victim] we believe you” you will be out of a job soon enough you filthy lying skank”.

39. On December 23, 2016, the victim received an email from weknow@hotdak.net with the message: “...give the world a great present and finish what you started 30 years ago...”

40. On January 2, 2017, the victim reported that the someone called Walgreens impersonating the victim’s primary care physician. The FBI interviewed the Pharmacist who took that call and confirmed an attempted call from someone who claimed they were with the ‘Office of [the victim’s doctor]’ and wanted to know details of medication for the victim. The caller hung up after the Pharmacist asked for more information regarding the Doctor’s office.

41. On January 5, 2017, the victim received an email from weknow@hotdak.net with the message: "...Attempt suicide lately skank?..."

42. On January 5, 2017, an email was sent from iama.skank@yandex.com to the victim's place of employment. The recipients of the email were the Managing Partner, the Operations Manager, and Office Manager. All individuals are in the direct chain of command over the victim. The message of the email was: "did [victim] tell you how pissed she was about her bonus? she mentioned both of you by name with some of her "friends" at other firms she doesnt even try to hide it [character return] according to [victim] she does more work than both of you combined, [Managing Partner]¹ is having an affair with some new lawyer and [employee name] is the office snitch [victim] has serious issues she should not be trusted go back and look at her outgoing emails before she deletes them [character return] if she denies any of this let me know and i will give you the names of the other people she has spoken to at the different firms she has serious psyc issues she has been making up stories about what is "happening" to her so she can get attention dont fall for it shes on psyc meds right now"

43. Following the delivery of the email above to the victim's chain of command, the FBI interviewed the victim and the victim's co-workers. The Operations Manager told the FBI that she had received three emails prior to the one on January 5, 2017; all three emails from the account weknow@hotdak.net (identified above). The victim told the FBI that Rosica had told her, while they were dating, that he had software on his laptop that would hide his identity.

¹ The names of the individuals referenced in the email are known to your Affiant but were withheld from this document to protect their identities.

44. Your Affiant believes that on or about January 17, 2017, Rosica created a new email account with the address weknow@mail2actor.com. Based, in part, on the email address itself, the content of subsequent emails, and the recipients of those emails, your Affiant believes that Rosica created all three emails accounts weknow@hotmail.net, iama.skank@yandex.com and weknow@mail2actor.com. Subpoena results from Mail2World for the email account weknow@mail2actor.com shows an account that was created on January 17, 2017 from IP address 171.25.193.131, believed by the Government to be a ToR node. Records of login activity for the weknow@mail2actor.com account identify activity from January 17, 2017 to February 12, 2017. The IP addresses associated with the account logins were all associated with ToR nodes.

45. On January 17, 2017, the victim received an email from weknow@mail2actor.com with the message "hey skank tell them the truth and they won't feel so sorry for you tell them the nasty things you have said about them the girls at the other firms know the same stuff we do you are a filthy lying skank". The victim's co-worker, Operations Manager at the law firm, was blind copied on the email. The victim received one additional email on January 17, 2017, four emails on January 18, 2017, and one email on January 19, 2017, and all emails were sent from weknow@mail2actor.com.

46. On January 31, 2017, the FBI obtained a Network Investigative Technique (NIT) Search Warrant on the user of email accounts: weknow@hotmail.net, iama.skank@yandex.com, and weknow@mail2actor.com. The purpose of the Search Warrant was to identify the user of the three email accounts. Prior investigation identified

the user of the accounts had been using ToR and / or proxy IP addresses; the Government believes this was done to hide the true identity of the user of the accounts. Execution of the Search Warrant involved sending emails to all three accounts with attachments and / or hyperlinks designed to return identifying information if and when those attachments or hyperlinks were accessed. The Search Warrant obtained approval to send a Microsoft Word attachment with an embedded image (described as the Embedded Image Option); this document when first opened prompted the user to perform an action in order to view the full content. If the receiver wanted to view the entire document they had to click exit 'protected view' which caused the computer to retrieve an image from an FBI owned computer. When the image was retrieved the logging of the FBI owned computer captured the IP address (outside of the ToR session) of the computer calling to retrieve the image. The Search Warrant also obtained approval to send a hyperlink via email (described as the Hyperlink Option); this hyperlink would be disguised in an email as a professional profile web page of the sender. If the receiver wanted to view the profile page of the sender they clicked on the link which took the user to a web page operated by the FBI. Logic on the web page stated that if the user was accessing the page from any IP address other than that of Rosica's home internet that an error page would be displayed saying this site was not accessible from a ToR or Proxy IP address. The FBI believed that Rosica would access the site from a ToR node first and then, upon seeing the error page, would access it from his home IP address (outside of the ToR session). Lastly, the Search Warrant obtained approval to send a Microsoft Excel attachment with embedded code (described as the Enable Macro Option) designed to return identifying information from the user's computer. This option required the user to open the

attachment and to click Enable Editing and Enable Content before the embedded code would execute and the computer would return the identifying information.

47. On February 2, 2017, the FBI executed the Embedded Image option from the NIT Search Warrant on the user of email accounts: weknow@hotdak.net, iama.skank@yandex.com, and weknow@mail2actor.com. The FBI facilitated the sending of an email from the victim's co-worker, the Operations Manager. This individual had just received a note from the weknow@mail2actor.com account at 2:58 PM. The Operations Manager replied to that email and copied iama.skank@yandex.com and weknow@hotdak.net. The email sent included a fictitious Cease and Desist Order within a Microsoft Word document. The email was sent at 3:10 PM. At 5:22 PM the server logs on the FBI owned computer showed the IP address 66.66.156.185 had retrieved the embedded image within the Microsoft Word document. The IP address in the server log matched the IP address provided from Time Warner Cable in a subpoena for the account of William Robert Rosica. Further, the IP address was identified by the FBI via monitoring of a Pen Register Trap and Trace of Rosica's home internet. Your Affiant believes that this information collectively identifies Rosica as the user of the email addresses weknow@hotdak.net, iama.skank@yandex.com, and weknow@mail2actor.com, and that Rosica accessed these accounts from his home internet service provided via Time Warner Cable.

48. On February 2, 2017 at 7:42 PM the Operations Manager received an email from the email account weknow@mail2actor.com with the subject line: ok. Content of the

email included the following, “we are not making any phone calls! she has someone doing it! we already told you this. she is a skank liar looking for drama. we will send no more emails. do youre home work. she is still shitalking you (she hates you) and [Managing Partner] and [Office Manager] and [co-worker]. her resume is all over the place and she is telling people she works for a corrupt firm. shame on you for beleiving her. if you only knew the level of her mentall illness”. The Government believes this was a direct response to the fictitious Cease and Desist Order requesting the Subject stop all incoming emails and phone calls to the business.

49. On February 6, 2017, at approximately 7:30 PM the victim notified the Affiant the she had just seen Rosica drive past her house. Later on February 6, 2017 at 9:20 PM the victim received an email to her personal Gmail account from weknow@mail2actor.com. In this email, the sender referenced a haircut the victim had received that evening; the victim later confirmed that she did travel from her home to get a haircut and returned home after. The victim received an additional email on February 7, 2017 at 12:21 PM from the same weknow@mail2actor.com account. At 6:34 PM on February 7, 2017 the victim received an email from skankcatcher@mail2actor.com. Your Affiant believes, based on previous actions and the content within the 6:34 PM email, that the user of weknow@mail2actor.com is the same user of skankcatcher@mail2actor.com. On February 13, 2017 the Honorable Jonathan W. Feldman, US Magistrate Judge with the Western District of New York, signed an amended NIT Search Warrant to include the new email address skankcatcher@mail2actor.com.

50. On February 16, 2017 the FBI executed the second phase of NTT Search Warrant; this phase sent both the Hyperlink and Enable Macro Options. At 2:35 PM the victim sent an email to weknow@hotdak.net, iama.skank@yandex.com, weknow@mail2actor.com, and skankcatcher@mail2actor.com. The email included the Microsoft Excel (Enable Macro Option) and a modification to the victim's traditional signature line including a new hyperlink to a fictitious professional profile page (Hyperlink Option).

51. On February 17, 2017, your Affiant reviewed footage from a pole camera less than two blocks away from the residence of the victim. Your Affiant focused the review on a window of time beginning at 7:15 PM to 7:45 PM on the evening of February 6, 2017; this was the approximate window provided by the victim when she saw Rosica drive by her residence. At 7:18 PM a silver / gray Chevy pickup truck was observed; the truck appeared to have four doors, tinted windows, and a cover across the truck bed. At 7:20 PM the Affiant saw, what appeared to be, the same silver / gray Chevy pickup truck drive through the pole camera viewpoint; in this footage the Affiant observed a running board under both side-doors. At 7:21 PM the Affiant saw, what appeared to be, the same silver / gray Chevy pickup truck drive through the pole camera viewpoint; in this footage the Affiant observed a half silver / half black side mirror.

52. Of February 17, 2017, your Affiant conducted physical surveillance at the employer of William Rosica. In the parking lot, a silver / gray Chevy Silverado pickup truck was identified with a covered truck bed, running board, and silver / gray side mirror. It is

your Affiant's belief that the vehicle observed through the pole camera was that of William Rosica and, that Rosica sent the email to the victim on February 6, 2017 at 9:20 PM after following her to get a haircut.

53. On February 19, 2017 the FBI reviewed logging of the web server hosting the pages for the Hyperlink Option. The logging showed that at 12:23:29 AM the IP address 51.15.58.152 accessed the web page of the Hyperlink Option; open source search of the IP address identified a ToR exit node. Approximately 30 seconds later at 12:23:56 AM the logging showed IP address 66.66.156.185 access the web page of the Hyperlink Option. The Government believes this is evidence that the user of one of the four email accounts receiving the email from the victim on February 16, 2017 accessed the fictitious professional profile page operated by the FBI, initially from within a ToR session and then from the home IP address of Rosica. Your Affiant believes this is evidence that Rosica is user of the previously identified email accounts and that he is responsible for creating these accounts in furtherance of his scheme to stalk the victim.


54. On or about January 25, 2017 the FBI initiated a Pen Register Trap and Trace (PRTT) on Rosica's home internet. This technique provided the FBI the authority to review internet traffic, without content, coming into and out of the IP address(es) associated with Rosica's home internet. Since the start of the home internet PRTT, the victim and victim co-workers received approximately 30 emails and observed four attempts to access the victim's work email account. On or about each of these dates and times (with the exception of two outgoing emails), the FBI observed corresponding ToR internet traffic into or out of Rosica's home IP address. The Government believes this is evidence that Rosica was online in a ToR

session at the same time all but two emails were received by the victim and co-workers as well as the times the victim's employer identified unauthorized email login attempts. More specifically, the Government believes Rosica would log in from his home Time Warner Cable internet, launch a ToR session to obfuscate his identity, and conduct activities associated with his scheme.

Conclusion

55. Based on the forgoing facts, my training and experience, and the information provided to me during the course of this investigation, I submit there is probable cause to believe that William Robert Rosica, has violated Title 18 U.S.C. §§ 2261A(1)(B), 2261A(2)(B), and 1030(a)(2)(C). Accordingly, I request that a criminal complaint and warrant be issued authorizing the arrest of William Robert Rosica.

Dated: Rochester, New York
March , 2017



KEVIN PARKER
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me
this 1 day of March, 2017.



HON. JONATHAN W. FELDMAN
UNITED STATES MAGISTRATE JUDGE